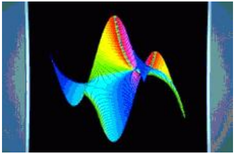
Fast compact solutions of linear differential or difference equations

Variants of some of S. Abramov's algorithms exploiting fast multiplication

Bruno Salvy

Algorithms Project, Inria



Joint work with A. Bostan, F. Chyzak and T. Cluzeau (ISSAC'05,06 and more)

Waterloo Abramov Workshop

I Introduction

Timings (I)

$$(2x+1)^3 y'' + (2x+1)(8x+3)y' + 2N((4x+2)N - 4x - 1)y = 0$$

has no polynomial solution ... but it takes time to detect this.

N	ABP	New	New
2^{12}	62.59	0.44	0.03
2^{14}	4597.2	2.40	0.07
2^{16}	$>$ 4Gb	14.67	0.19
2^{22}		3060.1	2.54
	$\tilde{O}(N^2)$	$\tilde{O}(N)$	$\tilde{O}(\sqrt{N})$
	deterministic		proba.

Timings (II)

$$S_m = \sum_n \binom{2n+m+N}{N} \binom{2m}{2n} \binom{m}{n} \quad \rightarrow \text{3rd order rec}$$

	Classical Zeilberger				Compact Z., random m			
N	$r=0$	$r=1$	$r=2$	$r=3$	$r=0$	$r=1$	$r=2$	$r=3$
2^4	0.1	0.2	0.3	0.6	0.1	0.3	0.9	2.5
2^5	0.3	0.7	1.5	3.4	0.1	0.5	1.4	5.1
2^6	2.9	6.8	12.	34.3	0.2	0.7	2.6	7.3
2^7	44.	131.	276.	1203.	0.3	1.5	5.0	15.2
2^8	1793.	$>$ 2Gb			0.5	2.7	11.3	35.5

deterministic — proba.

$\tilde{O}(N^4)$?

$\tilde{O}(N)$

symbolic m, det.: $\tilde{O}(N^2)$

II Matrix Factorials

Binary Splitting & Bit Complexity

Problem (Fast computation of $N! = 1 \times \cdots \times N$)

Naïve way: complexity $\tilde{O}(N^2)$

- Binary Splitting:

$$N! = \underbrace{(1 \times \cdots \times \lfloor N/2 \rfloor)}_{\text{size } \frac{1}{2} N \log N} \times \underbrace{((\lfloor N/2 \rfloor + 1) \times \cdots \times N)}_{\text{size } \frac{1}{2} N \log N}$$

  and recurse. Complexity $\tilde{O}(N)$.

- Extends to matrix factorials $C(N)C(N-1)\cdots C(1)$, same complexity $\rightarrow$ recurrences of arbitrary order.

[Hakmem72, Brent75, Chudnovsky^{2}88]

Baby-Steps/Giant-Steps

Problem ($N!$ mod p in less than N operations)

Naïve: N arithmetic operations

- Strassen 76: $\tilde{O}(\sqrt{N})$.
  1. Compute $Q(x) = (x+1)\cdots(x+k)$ — $\tilde{O}(k)$;
  2. Evaluate $Q(0), Q(k), \ldots, Q(N-k)$ — $\tilde{O}(N/k)$;
  3. Compute their product — $O(N/k)$.
- Extends to matrix factorials in $\tilde{O}(\sqrt{N})$ [Chudnovsky^{2}88];
- Fast extrapolation saves a log [BoGaSc03].

Application: dimension of kernel of $C(N)C(N-1)\cdots C(1)$ over $\mathbb{Q}$

Probabilistic algorithm in $\tilde{O}(\sqrt{N})$ bit operations [BoClSa05].

III Compact Representations

Solutions with Finite Support

Problem (Solutions such that $u_n = 0$ for all large n)

$$a_r(n)u_{n+r} + \cdots + a_0(n)u_n = 0.$$

- Upper end of finite support: largest integer root N of a_0;
- Undetermined coefficients $\rightarrow$

  $$u_0, u_1, \ldots, u_N, u_{N+1}, \ldots, u_{N+r-1} \text{ in } \tilde{O}(N^2) \text{ bit ops;}$$

- Matrix factorial $\rightarrow$ initial conditions in $\tilde{O}(N)$ bit ops and probabilistic test in $\tilde{O}(\sqrt{N})$.

Works for regular case ($0 \notin a_r(\mathbb{N})$) and irregular case (more technical).

Application: polynomial solutions

- Linear differential equation [BoClSa05]: linear recurrence on the coefficients;
- Linear difference equation [BoChClSa06]: same in the binomial basis [Boole1872,AbBrPe95].

Operations on the Compact Representation

Definition (Compact Representation)

Recurrence + initial conditions + bound N on support.

Data-structure of size $\tilde{O}(N)$ for a polynomial of size $\tilde{O}(N^2)$.

Lemma (Classical)

If u_n and v_n satisfy linear recurrences, so does $w_N := \sum_{n=0}^{N} u_n v_n$.

Corollary

P polynomial in compact representation, a algebraic number, then $P^{(k)}(a)$ can be computed in $\tilde{O}(N)$ bit operations (with $k = O(N)$).

Applications:

- $\exp(1), \gamma, \pi, \ldots$ [Hakmem,Brent,ChCh].
- Rational solutions of linear differential equations (gcd with $(x-a_1)^{N_1} \cdots (x-a_k)^{N_k}$) $\rightarrow$ quasi-optimal wrt solution.

IV Hypergeometric Summation

Abramov's Algorithm using Compact Representation (I)

Definition (Gosper-Petkovšek normal form)

$$\frac{P(n)}{Q(n)} = \frac{A(n)}{B(n)}\frac{C(n+1)}{C(n)}, \qquad \begin{cases} A(n) \wedge C(n) = B(n) \wedge C(n+1) = 1, \\ A(n) \wedge B(n+h) = 1 \quad (h \in \mathbb{N}). \end{cases}$$

deg C potentially exponential. Compact form via [Abramov95]:

$$\frac{C(n+1)}{C(n)} = \frac{g_1(n)}{g_1(n-h_1)} \cdots \frac{g_s(n)}{g_s(n-h_s)},$$

h_i's roots of the dispersion polynomial, g_i factors of P.

Theorem (Abramov 95)

The polynomial $C(n)$ of the Gosper-Petkovšek form of $(a_r(n-r+1), a_0(n))$ is a multiple of the denominator of all rational solutions of $a_r(n)u_{n+r} + \cdots + a_0(n)u_n = f(n)$.

Abramov's Algorithm using Compact Representation (II)

Rational solutions of LRE

$$a_r(n)u(n+r) + \cdots + a_0(n)u(n) = f(n).$$

1. Compute a compact representation of $C(n)$.
2. Change unknown: $u(n) = v(n)/C(n)$.
3. Homogeneous case ($f = 0$):
   reduce to same denominator and find polynomial solutions;
4. Non-homogeneous case (f non-zero polynomial):
   make homogeneous first. (Otherwise, rhs of expl degree.)

Corollary: Compact Gosper algorithm for indefinite summation.

Zeilberger's Algorithm using Compact Representation

Input: two rational functions $t_{n+1,m}/t_{n,m}$ and $t_{n,m+1}/t_{n,m}$
Output: linear recurrence $\sum_{i=0}^{r} \lambda_i(m) U_{m+i} = 0$ for $U_m = \sum_n t_{n,m}$.
For $r = 0, 1, 2, \dots$ while not found do

1. Construct (E_r) : $u_{n+1,m}\dfrac{t_{n+1,m}}{t_{n,m}} - u_{n,m} = \displaystyle\sum_{i=0}^{r} \lambda_i(m)\dfrac{t_{n,m+i}}{t_{n,m}}$;
2. Find if $\exists \lambda_1, \dots, \lambda_r \in \mathbb{Q}(m)$ s.t. solution $u_{n,m} \in \mathbb{Q}(n, m)$ via a linear system of size N in the λ_i's and the coeffs of numer(u).

Compact Version of Step 2

1. Take numerator of (E_r) and compute $C(n)$ compact multiple of denominator of sols;
2. Homogenize and change variable $u = v/C$ in this order;
3. This is not linear in the λ_i's. Linearity retrieved on subspace.
4. Compute system by matrix factorials. $(\to \tilde{O}(N^2))$

Can also be used for random $m \in \mathbb{Q}$ $(\to \tilde{O}(\sqrt{N})$ proba).

V Conclusion

Final Comments

- Thresholds to be found.
- Extensions to systems, to more general creative telescoping.
- In the difference case, gcd in compact representation?
- Presence of polynomial solutions in subexponential complexity?